

The specification has been objected to due to typographical errors. These typographical errors have been corrected.

The abstract of the specification has been objected to for containing the word “method”, which is alleged to be legal phraseology which allegedly is inappropriate. The same objection is made with respect to the title. Applicant respectfully submit that the word “method” is not legal phraseology (unlike the word “comprising”) and adequately describes Applicant’s invention. If the Examiner does not withdraw the objection, Applicant respectfully requests the support in the MPEP or 37 CFR Rules of Practice that would require Applicant to make such an amendment.

Claims 15-20 stand rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim Applicant’s subject matter due to a typographical error. Applicant has corrected the typographical error with respect to these claims.

Claims 1-5, 8-10, 12-17, 20-21 and 23-26 stand rejected under 35 U.S.C. §102(a) as being anticipated by the “SmartUpdate Developer’s Guide” dated March 11, 1999. The “SmartUpdate Developer’s Guide” describes from a software developer’s perspective, a mechanism for distributing and installing software over the internet and over intranets Java Archive Files (JAR files) is an installable file downloaded to a user’s machine in response to JavaScript used to trigger a SmartUpdate installation from a web page. A Client Version Registry is a cross platform registry that records all software installed through SmartUpdate and is stored on the user’s machine. Content creators can modify their pages to initiate an installation through SmartUpdate. Users can securely download or install or update software on their machines.

Once an installable JAR file has been published on the internet, content developers and end users may access it by initiating the SmartUpdate process in different ways. One way is to

provide an HTML page that contains a JavaScript trigger script. Another way is to provide a script that contains a direct link to the JAR file. Using a trigger class script, the Client Version Registry can be queried to see if the software is already installed as well as insuring that the installation be silent so that the user does not see dialog boxes during installation. SmartUpdate must be enabled on the user's machine in order for the trigger operation to work (see, for example, page 4 of chapter 6, "Decide Whether its Possible to Use SmartUpdate").

As to claim 1, the Office Action appears to equate a web browser with the claimed "first processing entity", the SmartUpdate "trigger" as the claimed second processing entity and the JAR file as the claimed third processing entity. However, Applicant respectfully notes that "a trigger" cannot be a processing entity as claimed since a trigger is merely a software code while a processing entity may be, for example, a server or computing device or other suitable processing device. In addition, a JAR file is simply a file and a computer file cannot be a "processing entity". Accordingly, the claims are believed to be in condition for allowance.

For argument sake, Applicant respectfully submits that the SmartUpdate reference does not teach or suggest, among other things, providing update complete data, under the control of the third processing entity, for the second processing entity. For example, Applicant's invention, among other advantages, notifies the second processing entity, which is the entity that determines that the update is required, that an update has been complete, by providing update complete data for the second processing entity so that the second processing entity knows that the update has been completed. The Office Action cites chapter 4, second paragraph, of the reference which describes that the client machine contains a Client Version Registry (CVR) which keeps track of the software which is accessed and modified by the server that provides the JAR file or by the server that installs the software. Hence, the first processing entity maintains

the CVR. The reference does not teach that the server that installs the software (i.e. the third processing entity) also provides updated complete data to the server (i.e. the second processing entity) that redirected the user to the third processing entity that updates the software. In fact, it appears that in the embodiment from the SmartUpdate reference, a server (e.g. the third processing entity) can query the Client Version Registry (stored in the first processing entity) to see if the software is the same or different to avoid duplicate installation. The client containing the CVR does not notify a redirecting server of its decision, but instead carries out the installation as needed. Accordingly, it appears that the only way the redirecting server (second processing entity) is aware that the software update has been completed, is that control is given back to the redirecting server. As such, the redirecting server does not analyze any data and does not access the Client Version Registry. As such, the Client Version Registry cannot be the equivalent of the update complete data as alleged in the Office Action. Accordingly, the claims are believed to be in condition for allowance.

Moreover, as noted in Applicant's specification on pages 8 and 9, for example, the third processing entity sends an update complete and redirect command back to the first processing entity for detection by the second processing entity. The update complete data and redirect command include, for example, a URL of the second processing entity along with data representing as the third processing entity cookie has been set in the first processor. The first processor then sends, for example, the URL of the second processing entity in a header with the data software cookie set equal to "yes" as provided by the third processing entity. As such, in one example, the third processing entity provides update complete data such as a cookie to indicate that the update was completed, for the second entity. The second entity analyzes this

data to determine that the update has been complete. Such an operation is not described or suggested in the cited reference.

As to claim 14, the Office Action rejects this claim for the same reasons given with respect to claim 1. As such, Applicant respectfully reasserts the relevant remarks made above and also submits that claim 14 is allowable. Moreover, the Office Action, on page 7, does not make clear which element within SmartUpdate is the third processing entity. In any event, Applicant also respectfully notes that claim 14 requires other limitations not present in claim 1. For example, Applicant claims detecting the need to update web certificate data for the web browser and providing web certificate update complete data as well as sending an universal resource locator associated with a processing entity to a web browser as claimed. The Office Action cites page 11, chapter 4, as describing detecting a need to update web certificate data. However, this portion merely indicates that signed Java classes may be used which are typically digitally signed objects or other information. There is no discussion of web certificates or a need to update web certificates as required by the claim. Accordingly, this claim is also believed to be in condition for allowance.

As to claim 2, Applicant respectfully submits that this claim is at least allowable depending from an allowable base claim.

As to claim 3, Applicant respectfully notes that this claim requires, among other things, providing update confirmation data from the first processing entity to the third processing entity in addition to the other limitations of claim 1. The Office Action indicates that it is inherent in that the first processing entity, which is allegedly a web browser and a third processing entity, which is allegedly the JAR file, would somehow require that the web browser must indicate the web browser status to the JAR file. However, this appears to be opposite of what the claim

requires and also is consistent with the cited reference. The claim requires that update confirmation data be provided from the first processing entity, such as a computer with a web browser, to a third processing entity such as a server that provides the updated web certificates or other software. The JAR file in the SmartUpdate reference is merely a file containing, among other things, the software to be updated. There is no discussion or need for that JAR file to be updated by the web server. To the contrary, it is the JAR file that is used to update the software on the computer that contains the web browser as described in the SmartUpdate installation reference. Accordingly, this claim is believed to be in condition for allowance.

As to claim 4, Applicant again notes, respectfully, that the method requires providing update complete data for the second processing entity, namely the processing entity that detects a need to update data for the first processing entity, by way of the first processing entity. In other words, the first processing entity must provide update complete data for the second processing entity. This is not disclosed in the cited reference. The Office Action cites chapter 4, page 6. However, this portion appears to indicate that after a script is complete, it may display a "README" file, and that if the installation changed a file that was in use by the operating system, the computer will need to be rebooted. There is no mention that the web browser provides update complete data for the trigger as alleged in the Office Action. Accordingly, this claim is also believed to be in condition for allowance.

As to claim 5, this claim is also believed to be allowable for the reasons set forth above with respect to claim 4.

As to claim 8, this claim requires, among other things, that automatically directing of communication is done based on update confirmation data. The Office Action indicates it would be inherent. However, the Office Action appears to be using different definitions of first and

second processing entities. In any event, Applicant respectfully notes that “update confirmation data” is different from “update complete data” as set forth in Applicant’s specification. As such, a first processing unit must generate update confirmation data indicating that confirmation data is sent from the first processing entity to the third processing entity (see, for example, page 8, lines 17-19 of Applicant’s specification). Applicant also respectfully submits that this claim is also allowable for the reasons set forth with respect to claim 1.

As to claims 9 and 10, Applicant respectfully notes that these claims include additional novel and nonobvious subject matter and are therefore also allowable.

As to claim 12, Applicant respectfully reasserts the relevant remarks made above with respect to claim 1.

As to claim 13, Applicant respectfully reasserts the relevant remarks made above with respect to claim 10.

As to claims 15-17 and 20-21, Applicant respectfully reasserts the relevant remarks made above with respect to claims 2-5 and 8-10.

Claims 6, 7, 11, 18, 19, 22 and 27 stand rejected under 35 U.S.C. §103(a) as being unpatentable over the “SmartUpdate” reference and in further view of U.S. Patent No. 6,209,093 (Venkatesan et al). The Venkatesan reference is directed to a technique for producing a privately authenticatable product copy indicia and for authenticating such indicia. For example, the indicia may be the access code attached to a cover of a CD ROM and during subsequent user installation of a copy to a computer, the user enters the indicia when prompted by the installation program, which in turn privately authenticates a signature contained in the indicia in order to continue or prematurely terminate the installation. The indicia is turned into an authentic

signature based on a public key crypto system. A third key is used in addition to conventional two public key crypto systems to give a unique product copy indicia.

As to claim 6, this claim requires, among other things, the step of detecting the need to update data for the first processing entity requires determining whether a connection request between the first and second processing entity includes the cookie associated with the second processing entity. The Office Action cites Venkatesan for teaching that cookies are used to communicate between two entities and that cookies can concern update information. However, Applicant respectfully notes that the Office Action appears to be reading additional disclosure into the cited reference. The cited portion of the reference, namely, column 14, line 41 to column 15, line 6, indicates that the cookie referred to therein is merely a representation of the installation number such as the indicia that contains the authentic signature so that the client's computer contains the indicia. The indicia is not update information. Moreover, Applicant's claim requires that the system detects whether an update is necessary based on whether a cookie is included in the connection request when the cookie is associated with the second processing entity. The indicia in Venkatesan is also not used to determine whether to update data. Such a method is not taught or suggested by the cited references and accordingly, this claim is also believed to be in condition for allowance.

As to claim 7, this claim requires, among other limitations, that the data being updated is certificate data and also requires determining whether a certificate update should occur based on whether cookies have been received by the first processing entity from both the second and third processing entities. As such, cookies must be placed by the second and third processing entities and analyzed by the first processing entity to determine whether a certificate update should occur. Applicant respectfully reasserts the relevant remarks made above with respect to the

Venkatesan reference and further notes that Venkatesan and the SmartUpdate reference are silent as to certificate update techniques as claimed and are also silent as to utilizing cookies from both the second and third processing entities as detected by the first processing entity as claimed. As such, Applicant respectfully submits that this claim is also in condition for allowance.

As to claim 11, this claim requires directing the update complete data to the second processing entity by using a redirect command back to the first processing entity as initiated by the third processing entity and in addition, sending a response to the update complete data, a cookie from the second processing entity to the first processing entity to confirm acceptance of the update. Applicant respectfully reasserts the relevant remarks made above with respect to the Venkatesan and also notes that there is no teaching or suggestion to combine the references. Moreover, even in combining the references, there is no teaching or suggestion of sending a cookie from the second processing unit to the first processing unit to confirm that acceptance of the update nor in providing updated complete data is done under the control of the third processing entity as claimed. Accordingly, this claim is also believed to be in condition for allowance. As previously noted, the SmartUpdate developer reference does not appear to provide any disclosure as to any closed loop system.

As to claims 18, 19 and 22, Applicant respectfully reasserts the relevant remarks made above with respect to claims 6, 7 and 11.

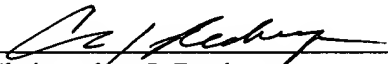
With respect to claim 27, Applicant respectfully reasserts the relevant remarks made above with respect to claims 6 and 7.

Attached hereto is a marked-up version of the changes made to the claims by the current amendment. The attached page is captioned "Version with Markings to Show Changes Made."

Accordingly, Applicant respectfully submits that the claims are in condition for allowance, and that an early Notice of Allowance be issued in this application. The Examiner is invited to contact the below-listed attorney if the Examiner believes that a telephone conference will advance the prosecution of this application.

Respectfully submitted,

Date: January 24, 2003

By 
Christopher J. Reckamp
Registration No 34,414

VEDDER, PRICE, KAUFMAN & KAMMHOLZ
222 N. LaSalle Street
Chicago, IL 60601
(312) 609-7599
FAX: (312) 609-5005

VERSION WITH MARKINGS TO SHOW CHANGES MADE

In the Specification:

Please replace the paragraph on page 5, beginning at line 22, and continuing on page 6, ending with line 3:

The systems and methods may be employed to update the software in different versions, provide unexpired root CA certificates, or provide any other suitable data. The system allows a user that has updated the root CA certificates to connect to a different site after upgrading wherein the different site detects if the data has already been upgraded or a new CA certificate downloaded to a web browser by detecting the universal cookie from the software update controller[]. For example, a first time through, a user []manually inserts the new root CA certificate in the web browser. The next time the user accesses a site that is in the program, it will be automatic. The different web servers cannot typically detect a 'universal cookie' of any sort. The browser gets a cookie and a special message **[[WHAT IS THE MESSAGE NAME IN THE FIGS?]]** encoded in the URL, or inserted into the HTTP headers, from the software update controller. The web server detects the special message in the URL or the HTTP headers, not in the cookie. The webserver then sets its own cookie for identification at a later date.

Please replace the paragraph on page 6, beginning at line 19, with the following rewritten paragraph:

Each of the second processing entities 104a-104n include a common gateway interface 108. Similarly, the third processing entity 106, configured as a software update controller, also includes a common gateway interface 110. The common gateway interfaces 108, 110 may be any suitable software modules, hardware circuits or any suitable combination thereof. A

common gateway interface, as known in the art of web servers, may include, for example, an external gateway program to interface with information servers such as HTTP servers, in compliance with the standard as may be found at Web address-
[http://]hooohoo.ncsa.uiuc.edu/cgi/overview.html.

In the Claims:

Please amend Claims 6 and 15-20 as follows. In particular, please substitute the below claims for the same claims with like number.

6. (Amended) The method of claim 1 [including] wherein the step of detecting a need to update data includes the step of determining whether a connection request between the first processing entity and the second processing entity includes a cookie associated with the second processing entity.

15. (Amended) The method of claim [10] 14 including the step of providing updated web certificate data for the web browser, by the processing entity in response to the redirected communication.[.]

16. (Amended) The method of claim [10] 14 including the step of providing web certificate update confirmation data from the web browser to the processing entity.

17. (Amended) The method of claim [10] 14 wherein the step of providing web certificate update complete data includes providing the certificate update complete data for the web server, by way of [[through]] the web browser.

18. (Amended) The method of claim [10] 14 including the step of determining whether a connection request between the web browser and the web server includes a cookie associated with the web server.

19. (Amended) The method of claim [10] 14 including determining whether a certificate update should occur for the web browser based on whether cookies have been received by the web browser from the web server and third processing entity.

20. (Amended) The method of claim [10] 14 including determining whether a certificate update should occur for the web browser based on whether cookies have been received by the web browser from the web server and third processing entity.